Open Integration Module

Highlights

See

- Discover devices the instant they connect to your network without requiring agents
- Classify and profile devices, users, applications and operating systems
- Assess device hygiene and continuously monitor security posture

Control

- Notify end users, administrators or IT systems about security issues
- Conform with policies, industry mandates and best practices such as network segmentation
- Restrict, block or quarantine noncompliant or compromised devices

Orchestrate

- Build integration between third-party products and the ForeScout platform to collapse existing information silos
- Share real-time information with existing security products and automate responses to mitigate threats and data breaches
- Improve overall security posture by automating routine activities and making better use of existing tools

The Challenges

Visibility. According to industry experts, a vast majority of successful attacks exploit well-known vulnerabilities and security gaps on managed endpoints and unmanaged devices. Most organizations are unaware of a significant percentage of the endpoints on their network because they are either not managed (personal systems, guest, and IoT/OT devices) have disabled or broken agents, or aren't detected by periodic scans (transient devices). As such, you are unaware of the attack surface on these devices.

Threat Detection. Today's cyberthreats are more sophisticated than ever and can easily evade traditional security defenses. Multi-vectored, stealthy and targeted, these attacks are focused on acquiring sensitive personal information, intellectual property or insider information. Compromised endpoints and data breaches can often remain undetected for weeks or months. To detect these advanced threats, zero-day attacks and infected endpoints, you need new security controls that do not rely on signatures.

Response Automation. The velocity and evasiveness of today's targeted attacks, coupled with increasing network complexity, mobility, BYOD, virtual instances, cloud adoption and IT/OT convergence, are creating the perfect storm for IT security teams. Without an automated system to continuously monitor and mitigate security gaps, valuable time is lost performing these tasks manually. And without the ability to automatically and quickly respond to attacks and security breaches, you are leaving the window open for cyberthreats to propagate within your network and exfiltrate data.

How it Works

The ForeScout platform includes physical or virtual network security appliance(s) that provide IT organizations with the unique ability to see devices, including non-traditional devices, the instant they connect to the network. It provides policy-based control of these devices, orchestrates information sharing and automates operation among disparate security and IT management tools.

The Open Integration Module allows customers, systems integrators and third-party product vendors to integrate homegrown applications or third-party products with the ForeScout platform. These bi-directional integrations enable third-party systems to:

- Consume information generated by the ForeScout platform, such as device type, compliance status, user information, operating system information, application information, peripheral information, physical layer information and more.
- Provide information to the ForeScout platform, such as host-related properties or events that can be used within a ForeScout policy.
- Receive or send action triggers to the ForeScout platform.

The Open Integration Module installs on the ForeScout appliance and allows it to send and receive information via the following open standards:

- **Web services.** The Open Integration Module can be configured to send and receive XML (Extensible Markup Language) formatted messages to a designated web service based on HTTP interaction. The communication uses REST (Representational State Transfer) web service requests and a simple XML format. The format of the messages is customizable and may contain ForeScout host properties. For example, the ForeScout platform can:
  - Update a firewall with up-to-date information about logged-in users and their current IP addresses. This allows the firewall to provide more accurate access rules.
  - Identify hosts that need remediation, based on company policies, and automatically open a new service ticket at the corporate help desk system.

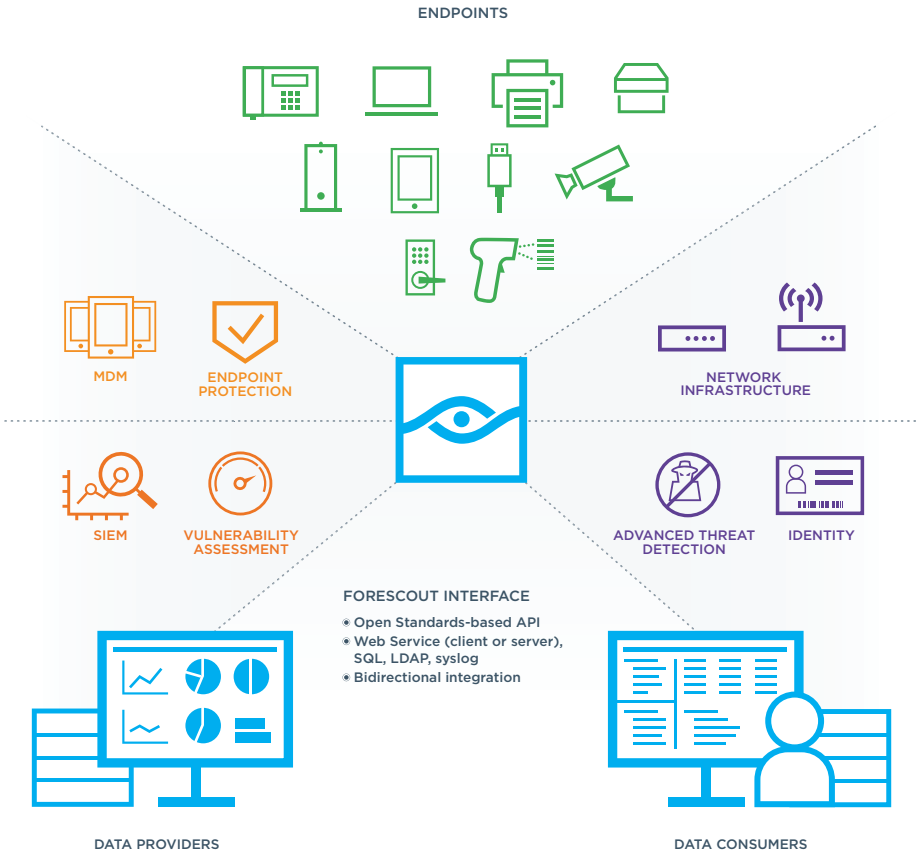

Figure 1: Information sharing with third-party products is made possible via the ForeScout interface.

- **SQL.** The ForeScout platform is able to push and pull information into and out of a standard SQL (Structured Query Language) database. This type of integration is common for interfacing with homegrown applications and with third-party products that are able to interface through an external or internal database. You can query external databases for information, and you can create host properties to store the data which the ForeScout platform retrieves. These host properties can be used in ForeScout

policies, and viewed in NAC and Inventory views. You can update external databases based on information gathered by the ForeScout platform, typically for some third-party product to act upon.

- **LDAP.** The ForeScout platform is able to generate custom queries to pull and push information into and out of a standard LDAP server. You can query the LDAP server for information, and create ForeScout host properties to store the data which has been retrieved. These host properties can be used in ForeScout platform policies, and viewed in NAC and Inventory views. Additionally, the following interface is included with the ForeScout platform:
- **Syslog.** The ForeScout platform can be configured to send and receive information via syslog to a designated server. This type of interface is used for a variety of integrations with products that aggregate logs, and enable log analysis, such as security information and event management products, or with other solutions that can send and receive alerts in this manner. The message format is customizable.

Learn more at
www.ForeScout.com

ForeScout

ForeScout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591